NO. 18-50440

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

LUKE WILSON,

Defendant-Appellant.

Appeal from the United States District Court
for the Southern District of California
Honorable Gonzalo P. Curiel, District Judge Presiding

APPELLANT'S OPENING BRIEF

DEVIN BURSTEIN
Warren & Burstein
501 West Broadway, Suite 240
San Diego, CA 92101
(619) 234-4433
Attorneys for Defendant-Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

Federal Statutes

Federal Rules

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. LUKE WILSON, Defendant-Appellant.	C.A. No. 18-50440 U.S.D.C. No. 15-cr-2838-GPC Southern District of California APPELLANT'S OPENING BRIEF

INTRODUCTION

In the district court's words, "we continue to have a novel and difficult legal issue of a first impression in the Ninth Circuit, which at this point the court continues to view as a significant question that there is a chance, a good chance, that the Ninth Circuit may see things differently than this court did. I have little doubt that at some point in the future, given artificial intelligence and the capabilities of artificial intelligence, the ruling that [I] issued will not be one that is recognized as being correct." ER:356.

The future is now.

There is no doubt the Fourth Amendment protects our mail from warrantless government intrusion. This Court and its sister Circuits have applied the same

principle to our electronic mail. The question here is whether that constitutional protection dissolves when a private company, like Google, reports an automated "hash" match between files in an email and previously flagged images of suspected child pornography. More specifically, does the hash match – which acts like a digital labeling system, but does *not* involve opening or viewing the contents of the email – allow law enforcement to search the contents of the email without a warrant?

We already have the answer. Under either a property-based or reasonable-expectation-of-privacy analysis, that search is unconstitutional. "The fact that the labels on the boxes established probable cause to believe the films were obscene clearly cannot excuse the failure to obtain a warrant; for if probable cause dispensed with the necessity of a warrant, one would never be needed." *Walter v. United States*, 447 U.S. 649, 657 n.10 (1980).

Here, as in *Walter*, it was federal agents, *not* a private party, who first opened and viewed the image files in Mr. Wilson's mail. "To be sure, the [hash of the images] gave them probable cause to believe that the [images] were obscene and that their shipment in interstate commerce had offended the federal criminal code. But the [hash] labels were not sufficient to support a conviction and were not mentioned in the indictment. Further investigation – that is to say, a search of the contents of the [images] – was necessary in order to obtain the evidence which was to be used at trial." *Id.* at 654. In short, "[p]rior to the Government screening, one could only

draw inferences about what was on the [images]. The [viewing] of the [images] was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search. That separate search was not supported by any exigency, or by a warrant even though one could have easily been obtained." *Id.* at 657.

Accordingly, the search was unconstitutional. Suppression should have followed. But the district court erroneously concluded there was no Fourth Amendment violation. Mr. Wilson's convictions resulted from that error. They cannot stand.

Separately, reversal is required because the district court failed to obtain a written jury waiver. *See* Fed. R. Crim. P. 23(a). Although there is a judicially created exception allowing oral waivers, the court here did not engage in the requisite thorough colloquy. It omitted several mandatory advisals, and confused the inquiry by coupling it with a discussion of evidentiary stipulations. Failure to obtain a valid waiver is structural error. So it was here.

JURISDICTIONAL STATEMENT

The district court had original jurisdiction over the criminal offenses under 18 U.S.C. § 3231. The court imposed sentence and filed an amended judgment and

commitment order on December 19, 2018. ER:440.[1] This was a final, appealable order. *See* 28 U.S.C. § 1291. The Notice of Appeal was timely filed on December 20, 2018. ER:414, 440; *see* Fed. R. App. P. 4(b). This Court has jurisdiction over a timely appeal from a final order entered in the Southern District of California. *See* 28 U.S.C. § 1291.

BAIL STATUS

Mr. Wilson is in custody serving concurrent federal and state sentences. His anticipated release date is unknown.

PERTINENT PROVISIONS

Pertinent statutory provisions appear in the attached addendum.

ISSUES FOR REVIEW

1. Whether the district court erred in denying Mr. Wilson's motion to suppress evidence obtained from the warrantless search of his email contents.

2. Whether the district court erred in failing to obtain a valid waiver of Mr. Wilson's right to a jury trial, as required by Federal Rule of Criminal Procedure 23(a).

[1] "ER" is the excerpt of record. Several pages are of poor quality, e.g., ER:32, but not those critical to this Court's review.

STATEMENT OF THE CASE

A. Email hashing: an overview.

Before turning to the facts, a technological synopsis is helpful. Companies like Google, Yahoo!, and AOL offer email accounts to their users. These electronic service providers (ESPs) have their own proprietary software that automatically scans every message, email, photo, movie, etc., on their system. ER:83.

Some of the data is used for marketing purposes – i.e., automatically generating targeted ads. ER:83. Other information goes to the government. As relevant here, Google provides information about suspected contraband image files found on its system. ER:79-80.

The process works as follows. Google (like other ESPs) has a private, proprietary database of hash values. ER:79. "A hash value is (usually) a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm — and calculated in a way that makes it highly unlikely another set of data will produce the same value." ER:189 (citation omitted). In simpler terms, it is a unique digital serial number assigned to a particular computer file – such that every copy of the file should have the same number (hash value) – which software can automatically recognize. ER:189.

As part of its database, Google assigns hash values to images its employees have previously identified as likely child pornography. ER:79-80. When such an

image is encountered – for instance, based on a customer report – a Google employee examines the image file and then its hash value is entered in Google's private database. ER:79-80.[2] The employee also enters an alphanumeric rating for each hashed image based on an employee's subjective interpretation: "A1" for a sex act involving a prepubescent minor; "A2" for a lascivious exhibition involving a prepubescent minor; "B1" for a sex act with a pubescent minor; and "B2" for a lascivious exhibition involving a pubescent minor. ER:98, 192.

Thereafter, because Google scans every email on its system,[3] if another file with the same hash value is embedded or attached to an email, Google will automatically detect it. ER:79-80. When this happens, the law (18 U.S.C. § 2258A(a)) requires Google to report the match to the CyberTipline of the National Center for Missing and Exploited Children (NCMEC). ER:187-88. In some instances – including this case – Google automatically generates an electronic report. ER:79-80. The report will contain basic information about the user's account, the suspect files in their original form (e.g., as image file attachments), and their alphanumeric rating. ER:192. However, a Google employee will *not* actually view

[2] Google does not keep a repository of the actual contraband images, as that would be illegal. It stores only the hash value. ER:79.

[3] The system is "Gmail," which has over a billion users. *See* Ross Miller, Gmail Now Has 1 Billion Monthly Active Users, The Verge (Feb. 1, 2016), http://www.theverge.com/2016/2/1/10889492/gmail-1-billion-google-alphabet.

the images to confirm whether they are child pornography, rather than a mistaken match. ER:80.[4]

Once the report reaches NCMEC, in some instances, a NCMEC employee will open the CyberTipline report to view the images. In other instances, *as in this case*, NCMEC will automatically forward the report electronically to a protected website accessible by law enforcement. ER:192-93. This happens without any NCMEC employee examining the images. ER:192-93. Law enforcement can then sign-on to the site, download, and print the report, including email contents (such as attached image files). ER:147. In this scenario, law enforcement is the first to open and view the email files. Before that happens, no human at either Google or NCMEC has confirmed what the images depict. That is the scenario here. ER:193.

B. Google's automated hashing of Mr. Wilson's email and the government search that followed.

Mr. Wilson sent an email containing four image files from his Gmail account (soulrebelsd@gmail.com) to an acquaintance. ER:191. Google's software automatically scanned the email. ER:80. Without any human involvement, the software detected a "hash" match between the image-file attachments and other previously identified images of likely child pornography. ER:80.

[4] Other times, a Google employee will examine the image before sending the report to NCMEC, but that did not happen here. ER:80.

Google automatically generated and sent an electronic CyberTipline report to NCMEC, which included the image files identified as email attachments and an "A1" classification. ER:80, 95, 157. The report indicated that a Google employee did *not* review the images. ER:80, 157. NCMEC then electronically forwarded the CyberTipline Report to a site accessible by law enforcement; specifically the San Diego Internet Crimes Against Children Task Force. NCMEC made clear the files were "unconfirmed." ER:101. Like Google, it had "not opened or viewed any uploaded files submitted with this report and has no information concerning the content of the uploaded files other than information provided in the report by the ESP." ER:101.

Thereafter, the Task Force downloaded, opened, and printed the report it received from NCMEC, including the four image-file email attachments. ER:147-48, 153-54. Special Agent William Thompson was the first person to view the images that Mr. Wilson had emailed a few days earlier. ER:158-59.

Agent Thompson confirmed the images were child pornography, and sought a search warrant for Mr. Wilson's email account. ER:106, 150. The warrant application relied on the information gained from opening the email attachments to establish probable cause. ER:62, 106-08 151. The subsequent search resulted in

additional incriminating evidence. ER:7.[5] Agent Thompson then sought a search warrant for Mr. Wilson's home, which again relied in part on the CyberTipline Report. ER:7. During the search, agents found additional child pornography images. ER:7, 65.

C. The denial of Mr. Wilson's motion to suppress.

The government filed a three-count indictment charging Mr. Wilson with: (1) advertising child pornography; (2) distributing child pornography; and (3) possessing child pornography. ER:1-4.

1. The motion to suppress.

Mr. Wilson moved to suppress the evidence. ER:5. He argued, "the government violated [his] constitutional rights under the Fourth Amendment when, without seeking a warrant, the agent opened [his] private email and the attached files and viewed their contents . . . . For that reason, the fruits from the tainted initial search in this case must be suppressed." ER:8.

The motion further explained, "Mr. Wilson had a Fourth Amendment property interest in his electronic mail, and that property interest existed until his mail reached its intended recipient – which it never did because it was intercepted by Google.

[5] Agents also found messages in which Mr. Wilson communicated with a woman about filming herself engaged in sexual conduct with minors and sending the images to Mr. Wilson. ER:7. Those messages resulted in state-court criminal charges that are irrelevant to this appeal.

Because the government searched the mail prior to its delivery, the search implicated the Fourth Amendment. Moreover, the search implicated the Fourth Amendment because Mr. Wilson had a subjective expectation of privacy in his email, and that subjective expectation of privacy was objectively reasonable." ER:9. "Thus, under either . . . theory, the government conducted a warrantless search in violation of the Fourth Amendment when it opened Mr. Wilson's email[.]" ER:12.

Additionally, Mr. Wilson's motion explained that the government could not rely on any exception to the exclusionary rule. The good faith exception did not apply because Agent Thompson did not rely on any statute or appellate precedent authorizing a warrantless search. ER:12-13. Nor could the government rely on the inevitable discovery or independent source doctrines. ER:14-16. And because the initial search warrant relied on the unconstitutionally-obtained information from Agent Thompson's search to establish probable cause, it too failed. ER:16-17. Thus, all evidence was fruit of the poisonous tree. ER:18.

2. The government's response.

The government opposed the motion, relying primarily on the private search doctrine. ER:67.[6] It argued that, based on Google's hashing software, "[l]aw enforcement's viewing of the images – after it received the CyberTipline report from NCMEC – did not constitute an expansion of Google's [private] search, and the evidence should not be suppressed." ER:68.

The government further claimed that, "[e]ven if the Court finds that viewing the four images violated Fourth Amendment protections, the evidence should not be excluded" because the agents acted in "good faith." ER:68-70. Finally, the government argued that, based on Google's terms of service agreement, Mr. Wilson did not have a reasonable expectation of privacy in the images. ER:73. The government did not address Mr. Wilson's property-based claim.

3. The district court's decision.

The district court held an evidentiary hearing on the motion. Agent Thompson testified consistently with the facts set forth above. He also explained that Google's

[6] The doctrine is an exception to the warrant requirement. As discussed in more detail below, it works as follows: When a private party conducts a search there is no Fourth Amendment violation. The government can then piggyback on the private search to conduct a coextensive search without a warrant, because it does not further frustrate the individual's expectation of privacy; the private search has already accomplished that frustration. On the other hand, if the government expands the scope of the private search, that expansion violates the Fourth Amendment. *See United States v. Jacobsen*, 466 U.S. 109, 115 (1984).

hashing system is propriety. ER:163. Thus, even if Google provided the government with the exact hash value of an image it flagged as likely child pornography, Agent Thompson "wouldn't be able to compare that against law enforcement's hash value databases[.]" ER:163. In that case, "[t]here would have to be some additional work to kind of fix that issue." ER:163. In other words, the government could not recreate the image from Google's hash value alone. ER:163.

Following the hearing, the district court denied the motion. ER:187. Based on Google's terms of service, the court doubted whether Mr. Wilson had an "objectively reasonable expectation of privacy in the four child pornography files he uploaded to his Google email account." ER:199. But the court did not rely on this ground: "In any event, the Court's resolution of the instant motion to suppress does not depend upon the finding that Defendant lacked an expectation of privacy in the four child pornography files he uploaded to his Google email account." ER:200. "To be clear, the Court *does not reach the question* of whether Defendant's expectation of privacy in the contents of his Google email account was extinguished across the board by his agreement to Google's Terms of Service." ER:200 n.7 (emphasis added).

Instead, the "decision rest[ed] upon the conclusion that [under the private search doctrine] the government did not significantly expand upon Google's private search." ER:200. The court supported its decision by inventing a constitutionally

significant distinction between an email (presumably its text) and the embedded or attached image files. ER:192 ("Google did not forward the email itself to NCMEC"); ER:193 ("SA Thompson's review was limited to the contents of the CyberTipline Report and the four image files. He did not view or have access to Defendant's email at this time."); ER:200 n.7 ("SA Thompson never viewed the contents of Defendant's email without a warrant—he viewed only the four child pornography photographs Defendant uploaded.").[7]

The court then determined, "the use of hashing technology to identify illegal files like child pornography certainly constitutes a search." ER:204. Thus, "Google's use of its proprietary hashing technology to screen Defendant's email account constituted a private search." ER:204. But "even assuming arguendo that SA Thompson's viewing of the four images was an expansion of Google's private search, it was not a significant expansion." ER:204-05.

The court continued, because "SA Thompson already knew, before visually examining the images, from the 'A1' classification that each of the four images depicted a prepubescent minor engaged in a sex act," there was a "virtual certainty

[7] The district court seems to have misunderstood that, just like physical mail may contain a letter, card, photos, and/or other documents, the same is true of an email. All contents of the envelope – whatever is included – are protected. And this principle also applies to email. Thus, the district court's analytical separation of the images from the email was misguided.

[he] could learn nothing that had not previously been learned during the private search." ER:205 (internal citations and quotations omitted).

After concluding there was no Fourth Amendment violation, the district court considered, and rejected, the government's alternative arguments. First, it found that "excising the tainted evidence from the affidavit would not support issuance of the search warrant for Defendant's email account." ER:207. Second, it held, "if SA Thompson's warrantless viewing of the four images constituted an illegal search, the good faith exception would not apply to prevent operation of the exclusionary rule." ER:208-09. Because "SA Thompson made the [alleged] constitutional error in this case[,] [t]he magistrate's issuance of the warrant and consideration of the evidence would not 'sanitize the taint of the illegal warrantless search.' An illegal warrantless search would be precisely the sort of conduct the exclusionary rule was meant to deter." ER:209 (citation omitted).

The court summarized its ruling as follows: "if SA Thompson's warrantless viewing of the four images constituted an illegal search, neither excising the tainted evidence from the affidavit nor the good faith exception would prevent operation of the exclusionary rule. Nevertheless, as detailed above, [] SA Thompson's visual examination of the four images did not significantly expand upon Google's private search, and thus did not constitute a search within meaning of the Fourth Amendment." ER:209.

D. The jury waiver and conviction.

Before trial, the parties agreed to several evidentiary stipulations and also indicated they would waive the jury. ER:213-14, 226-27. The court asked Mr. Wilson about both issues at the same time:

Court: I understand that you are prepared to waive your right to a jury trial. Is that correct, sir?

Wilson: Yes, Your Honor.

Court: All right. So you understand that you have a right to have the government present this case to a jury and then for the jury to consider whether or not they have met their burden of proof on each of the elements of each of the three offenses that have been charged in this case. Do you understand that?

Wilson: Yes. We're not dealing with a jury, though. Correct?

Court: No. Do you understand that you have that right?

Wilson: Yes, I do understand.

Court: All right. And if this case went to trial, you would have the right to have the jury decide whether or not you're innocent or guilty.

Wilson: Yes, Your Honor.

Court: And in terms of finding guilt, it's required, it would be required that all 12 jurors find you guilty. Do you understand that?

Wilson: Yes.

Court: And at the trial you would have a right to have the government establish their case with proof beyond a reasonable doubt on each of the elements of the three offenses. Do you understand that?

Wilson: Yes, Your Honor.

Court: All right. Along with that, you have the right to have the government call each of their witnesses to testify and then for you to cross-examine each of the witnesses. Do you understand that?

Wilson: Yes.

Court: All right. So, in this case, you still have the right to have the government prove their case with evidence beyond a reasonable doubt. That's still baked into this process, but at this time I understand that the parties are agreeable to having certain facts stipulated to. Do you understand that?

Wilson: Yes.

Court: So, as to those facts that you're stipulating to, normally, those would be established by the government calling a witness, having them placed under oath and testifying, and then Mr. Kirby would be able to cross-examine each and every witness called by the government. Do you understand that?

Wilson: Yes, Your Honor.

Court: All right. And so at this time, as I understand it, you intend to waive the right to cross-examine any of the witnesses that the government would otherwise have been presenting.

Wilson: Yes, Your Honor.

ER:218-220.

After the colloquy, the prosecutor stated the minimum and maximum penalties for each charge. ER:221. The district court then asked: "Do you have any questions about anything that I have gone over, your constitutional rights that you would otherwise be waiving by entering the stipulated-facts portion of this

proceeding, or anything else?" ER:223. Mr. Wilson indicated he understood. ER:223. And the court concluded, "Mr. Wilson has waived his right to a jury trial, and so we can proceed with a bench trial." ER:224. The parties then filed a stipulation of facts, but not a written jury waiver. ER:226-27.

Approximately two weeks after taking the oral waiver, the court held a bench trial. ER:230. The court confirmed the factual stipulations with Mr. Wilson, ER:231-32, but did not inquire as to whether he wanted to proceed without a jury. Nor did the court ask for a written jury waiver.

During the bench trial, the government introduced evidence derived from the search warrants showing Mr. Wilson possessed and distributed child pornography. ER:235-308. The district court convicted him of those charges (counts two and three), and the government dismissed the advertising charge (count one). ER:323-35. The district court initially imposed a 13-year sentence. ER:350. Mr. Wilson appealed.

Thereafter, the defense learned the government failed to provide a material piece of evidence in discovery. Based on that failure, the parties jointly moved to vacate the sentence and remand the case to the district court for resentencing. *See* Case No. 18-50088, Dckt. No. 6. This Court granted the motion. *See id*. at Dckt. No. 7. On remand, the district court cut the sentence to 11 years, and ran it concurrent with a previously imposed state court term. ER:416.

During the pendency of the proceedings, the district court also had an opportunity to reflect on the basis for its suppression ruling. As noted above, it said: "there is a chance, a good chance, that the Ninth Circuit may see things differently than this Court did. I have little doubt that at some point in the future . . . the ruling that [I] issued will not be one that is recognized as being correct." ER:356.

Indeed, it was not.

SUMMARY OF ARGUMENT

This Court should reverse the district court's denial of Mr. Wilson's motion to suppress. By opening and reviewing Mr. Wilson's email contents without a warrant, the government violated his Fourth Amendment right to be secure in his papers. Under this property-based theory, the district court's reliance on the private search doctrine was misplaced. That doctrine serves *only* to frustrate a defendant's reasonable expectation of privacy. It cannot overcome, diminish, or impede a Fourth Amendment trespassory claim.

Moreover, even as to Mr. Wilson's expectation of privacy, the private search doctrine cannot shield the government's warrantless review from constitutional scrutiny. This is so for three reasons.

First, Google's automated hashing process was not a private "search." It was the modern equivalent of a "sniff" by a drug dog, capable *only* of identifying specified contraband. Under binding Supreme Court precedent, because a dog-sniff

is merely a non-invasive contraband determination, it does not frustrate any valid privacy interest. So too of Google's automated hashing technology. And with no private "search" on which to piggyback, the private search doctrine is inapplicable. The government's conduct was the initial constitutionally significant act.

Second, even if hashing could be considered a "search," the private search doctrine does not apply to automated, non-human actions. The point of the doctrine is that the government agent does nothing more than recreate what the private person did, and thus does not further invade the individual's privacy. That rationale falls apart, however, when the private action has no privacy implication. Here, because the hashing and reporting was automated, no Google employee learned anything about Mr. Wilson's email. As such, there was no initial privacy breach on which the government could piggyback.

Third, even if Google's hashing could trigger the private search doctrine, the district court got it wrong. The court's conclusion that opening and viewing the image files was not a significant expansion on the hash comparison is easily disproven. As Agent Thompson conceded, the government could not have used Google's hash values to generate the images. Nor did the hash value tell the government anything about the gender, race, ethnicity, or sex of the person or people in the images. It could not even tell how many people were depicted. And of course,

a prosecutor could not waive a hash value in front of the jury, or use it to obtain a conviction.

In short, just like an old Dewey-decimal card is not the library book, the hash is not the image. If Google printed out the hash value on a piece of paper and handed it to Agent Thompson, he would not be holding a picture. He would merely have in his hand Google's filing number for the image. Only by opening the library book can its contents be read. And only by opening an image file can its contents be seen. That is a search under the Fourth Amendment.

The district court was also misguided in suggesting Google's terms of service rendered Mr. Wilson's expectation of privacy unreasonable. Its opinion on the matter runs into a wall of contrary precedent. And it defies the common experience. Gather any ten people and ask how many read the fine print of Google's terms of service before signing on. Nary a hand will be raised.

In any event, even if someone took out the magnifying glass, what he or she would find is Google's commitment that what you put on the platform remains your property. Thus, if the terms of service can diminish the expectation of privacy, they must concurrently buttress the user's property rights. Here, that is outcome-determinative in favor of Mr. Wilson's trespass claim.

This leaves only the issue of remedy. But the Court's precedent answers that question too. Because everything flowed from Agent Thompson's initial Fourth

Amendment violation, the exclusionary rule applies. As stated in *United States v. Vasey*, 834 F.2d 782, 789-90 (9th Cir. 1987), there is no exception for "evidence seized during a search under a warrant if that warrant was based on evidence seized in an unconstitutional search." Accordingly, Mr. Wilson's convictions cannot stand.

Separately, reversal is also required because the district court erred in failing to obtain a written waiver of Mr. Wilson's right to a jury trial, and its oral colloquy was insufficient. Therefore, at a minimum, the Court should remand for a new trial.

ARGUMENT

I.
The district court erred in denying Mr. Wilson's motion to suppress.

A. Standard of review.

The Court reviews "a district court's denial of a motion to suppress evidence de novo, and the district court's underlying factual findings for clear error." *United States v. Job*, 871 F.3d 852, 859 (9th Cir. 2017).

B. The government conducted a warrantless search of Mr. Wilson's email contents.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. It is triggered in two circumstances. First, there is a "search" within the meaning of the Fourth Amendment when the government intrudes or trespasses upon a constitutionally protected area – "persons, houses,

papers, [or] effects" – "for the purpose of obtaining information." *United States v. Jones*, 565 U.S. 400, 404 (2012). Second, a "search" occurs when a government agent infringes on "an expectation of privacy that society is prepared to consider reasonable[.]" *Jacobsen*, 466 U.S. at 113; *see also Jones*, 565 U.S. at 409 (the "reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.").[8]

Mail and its electronic counterpart, email, implicate both Fourth Amendment considerations – property and privacy.

1. The contents of email are constitutionally protected.

a. *Like physical mail, the Fourth Amendment protects a user's property interest in the contents of his or her email.*

Beginning with traditional property principles, in *Ex Parte Jackson*, 96 U.S. 727, 733 (1877), the Supreme Court held, "[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." It further explained, "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst

[8] The reasonable expectation of privacy test is often referred to as the *Katz* test, because that is the case in which the theory originated. *See Katz v. United States*, 389 U.S. 347 (1967).

in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household." *Id.*

This is equally true of email. As the Court held in *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc), "[email] implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.' The express listing of papers 'reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas — what we might call freedom of conscience — from invasion by the government." (Citation omitted).

In other words, "an email is a 'paper' or 'effect' for Fourth Amendment purposes, a form of communication capable of storing all sorts of private and personal details, from correspondence to images, video or audio files, and so much more." *United States v. Ackerman*, 831 F.3d 1292, 1304 (10th Cir. 2016) (citing *Cotterman*, 709 F.3d at 964).

Thus, when a government agent opens and views the contents of an email without a warrant, "that seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." *Id*. at 1307. And while "the framers were concerned with the protection of physical rather than virtual correspondence[,] a more obvious analogy from principle to new technology is hard to imagine and, indeed, many courts have

already applied the common law's ancient trespass to chattels doctrine to electronic, not just written, communications." *Id*. at 1308 (listing cases).

b. *Like physical mail, the Fourth Amendment protects a user's privacy interest in the contents of his or her email.*

Separately, as noted, there is a protected privacy interest in email. "E-mail, like physical mail, has . . . a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical." *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008). Thus, "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial [E]SP." *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (internal quotations omitted); *see also Grand Jury Subpoena v. Kitzhaber*, 828 F.3d 1083, 1090 (9th Cir. 2016) ("emails are to be treated as closed, addressed packages for expectation-of-privacy purposes.").

Succinctly stated: "With respect to . . . privacy interest, we treat emails as letters. Accordingly, until electronic communications reach the recipient, they retain the same level of privacy interest as if they were still in the home." *United States v. Mohamud*, 843 F.3d 420, 442 (9th Cir. 2016) (citation omitted). And given that the home is "the most constitutionally protected place on earth," *United States v.*

Craighead, 539 F.3d 1073, 1083 (9th Cir. 2008), email enjoys heightened Fourth Amendment protection.

Thus, whether the "search" question is analyzed "through the [reasonable expectation of privacy] lens . . . or through the lens of the traditional trespass test[,] they yield the same (and pretty intuitive) result: [the government] conduct[s] a 'search' when it open[s] and examine[s] [] email." *Ackerman*, 831 F.3d at 1308.

2. The government violated the Fourth Amendment by opening and viewing the contents of Mr. Wilson's email without a warrant.

Applying these principles here leads to a simple (and pretty intuitive) conclusion: opening and viewing the contents of Mr. Wilson's email was a search under the Fourth Amendment.

a. *The government violated Mr. Wilson's Fourth Amendment property rights*.

The contents of the email were Mr. Wilson's property – his papers or effects. Just like the package in *Ex Parte Jackson,* 96 U.S. at 733, no one possessed a superior ownership interest. Indeed, by its own admission, "'Google does not claim *any ownership* in any of the content, including any text, data, information, images, photographs, music, sound, video, or other material, that [users] upload, transmit or store in [their] Gmail account.'" *In re Google Inc. Gmail Litig*., 2014 U.S. Dist. LEXIS 36957, *16 n.4 (N.D. Cal. 2014) (citation omitted, emphasis added); *see also* Google Terms of Service, https://policies.google.com/terms ("Some of our Services

allow you to upload, submit, store, send or receive content . . . . In short, what belongs to you stays yours.").

To this end, "few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest." *Carpenter v. United States*, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, J. dissenting); *see also Ajemian v. Yahoo!, Inc.*, 478 Mass. 169, 170 (2017) (an email account is a "form of property often referred to as a 'digital asset'"); *United States v. Kernell*, 2010 U.S. Dist. LEXIS 36477, *13-15 (E.D. Tenn. 2010) (an individual has a property right to the exclusive use of the information and pictures contained in her email account). Thus, "[i]t did not matter that [Mr. Wilson's emails] were bailed to a third party[.]. The sender enjoyed the same Fourth Amendment protection as he d[id] 'when papers are subjected to search in one's own household.'" *Carpenter*, 138 S. Ct. at 2269 (quoting *Ex parte Jackson*, 96 U.S. at 733).

Agent Thompson violated that protected legal interest. It was as if he opened private mail in Mr. Wilson's home for the purpose of obtaining incriminating information. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("obtaining by [] technology any information [from] the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search[.]") (citation omitted). This was the modern equivalent of

a common law trespass. *See id.; Jones*, 565 U.S. at 419 n.2 ("At common law, a suit for trespass to chattels could be maintained if there was a violation of the dignitary interest in the inviolability of chattels") (Alito, J., concurring) (internal quotations and citation omitted). And because "the Fourth Amendment is no less protective of persons and property against governmental invasions than the common law was at the time of the founding," this trespass violated the Fourth Amendment. *Ackerman*, 831 F.3d at 1307.

b. *The government violated Mr. Wilson's Fourth Amendment privacy rights.*

The same conclusion follows under the *Katz* test. In *Katz*, the Supreme Court formulated a Fourth Amendment test based on whether a person has a "reasonable expectation of privacy," a concept that imposes "a twofold requirement, first that the person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" 389 U.S. at 361 (Harlan, J., concurring).

Here, there is no doubt Mr. Wilson had a subjective expectation of privacy in the contents of his email. ER:53 (Mr. Wilson: "I believed that my communications using that email account were private. [] I thought that any emails or other information I sent to others was private."). That point is not in dispute. ER:199 (district court: "Defendant held a subjective expectation of privacy in his Google

email account at all relevant times"). It is equally clear that his expectation of privacy was one that society is prepared to recognize as reasonable.

As this Court explained in *Kitzhaber*, "emails are to be treated as closed, addressed packages for expectation-of-privacy purposes. And a person does not forfeit [his] expectation of privacy merely because [a private] container is located in a place that is not controlled exclusively by the container's owner." 828 F.3d at 1090 (internal quotation and citations omitted). As such, "emails," are "records [that] are expected to be kept private and this expectation is one that society is prepared to recognize as reasonable." *Id*. (internal quotation and citations omitted); *see also Warshak*, 631 F.3d at 288 (subscribers have an objectively reasonable expectation of privacy in their emails); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904 (9th Cir. 2008) (users have a reasonable expectation of privacy in text messages), *rev'd on other grounds*, 560 U.S. 746 (2010).

In short, as a matter of both property and privacy, in opening and viewing the contents of Mr. Wilson's email, the government violated the Fourth Amendment.

Nor is it constitutionally significant that the agent did not access or read the text component of the email. There is no basis to distinguish the image-file attachments from the email's text. By way of example, consider an envelope containing a letter along with photos. If a government agent intercepted the mail, viewed the photos, but did not read the letter, the act would still offend the Fourth

Amendment. *See Jacobsen*, 466 U.S. at 114 ("Even when government agents may lawfully seize [] a package . . . the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package").

The same principle applies to email. Attachments – anything from medical records and business plans to photographs – implicate the identical privacy and property interests. They have the same protection as the text: "Consider an email attachment containing sensitive personal information sent from a secure Wi-Fi network to a doctor, lawyer, accountant, priest, or spouse. A company like Google that intercepts the contents of that email from the encrypted home network has, quite understandably, violated the Wiretap Act." *Joffe v. Google, Inc.*, 746 F.3d 920, 931 (9th Cir. 2013). And an agent who opens and views the contents of that email, as Agent Thompson did, has violated the Fourth Amendment.

C. The district court's misapplication of the private search doctrine.

The district court concluded otherwise. In its view, Agent Thompson's conduct did not infringe on any constitutionally protected interest, because he did not meaningfully expand on Google's private search. This is incorrect. First, the private search doctrine does not apply. Second, even if it did, Agent Thompson unconstitutionally exceeded the scope of Google's automated hash match.

1. The private search doctrine has no impact on Mr. Wilson's property-based Fourth Amendment claim.

At the outset, given Mr. Wilson's property-based claim, the private search doctrine is much ado about nothing. It has no application in the Fourth Amendment *trespass* context. The rationale underlying the doctrine is that the private party frustrates the reasonable expectation of privacy by exposing the object of the search and "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information[.]" *Jacobsen*, 466 U.S. at 117.

But as then-Judge Gorsuch explained in *Ackerman*, 831 F.3d at 1307, a person may continue to have a protected *property* interest in his or her papers and effects, without a concomitant *privacy* interest. This is because entrusting property – be it a package or data – to a private party creates a bailment. *See id.* Under that arrangement, the bailor does not forfeit any property right in that item vis-à-vis another third-party, like the government. *See Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J. dissenting) ("just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it") (emphasis in original).

Indeed, that is precisely what the Supreme Court recently decided in *Carpenter*. There, it did not matter that a third party held the defendant's electronic

location information; that data was still protected from warrantless government intrusion. *Carpenter*, 138 S. Ct. at 2223 (majority opinion).

The same is true here. Although Mr. Wilson entrusted his electronic property to Google, it was still protected from warrantless government intrusion (trespass). Accordingly, Mr. Wilson can and should prevail in this appeal under his Fourth Amendment property claim, regardless of whether the private search doctrine would otherwise undermine his reasonable expectation of privacy.

This Court, therefore, need not reach the privacy issue. But if it does, the Court should find the private search doctrine inapplicable.

2. The private search doctrine is inapplicable because Google's automated hash screening was not a "search."

The district court concluded, "Google's use of its proprietary hashing technology to screen Defendant's email account constituted a private search." ER:204. Not so. As used here, Google's automatic hash screening could not frustrate Mr. Wilson's reasonable expectation of privacy, and thus did not qualify as a private search under the Fourth Amendment. As such, it could not serve as the basis for the government's subsequent search of the image files. In short, because there was no private search, the private search doctrine cannot apply.

a. *Google's automated hashing is not constitutionally different than a dog-sniff.*

Google's hashing of Mr. Wilson's email was the functional equivalent of a technological dog-sniff. Like a narcotics detector dog, the hashing software had – and could accomplish – only one, limited objective; to identify the presence of suspected contraband on which it was previously trained without the need to open the package (email) and examine its contents.

Under *United States v. Place*, 462 U.S. 696 (1983), that is not a search. In *Place*, the Supreme Court considered the constitutional implications of exposing personal luggage to a narcotics detector dog. *See id*. at 706-07. Although it recognized a "privacy interest in the contents of personal luggage that is protected by the Fourth Amendment," it found that "exposure of respondent's luggage . . . to a trained canine [] *did not constitute a 'search*' within the meaning of the Fourth Amendment." *Id.* at 707 (emphasis added).

The Court reasoned: "A 'canine sniff' by a well-trained narcotics detection dog [] does not require opening the luggage. It does not expose noncontraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage. Thus, the manner in which information is obtained through this investigative technique is much less intrusive

than a typical search. Moreover, the sniff discloses only the presence or absence of narcotics, a contraband item." *Id*.

When *Place* was decided in 1983, the Court was "aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure." *Id.* Much has changed. And hashing, at least as Google used it here, is not materially different than the dog-sniff in *Place*.

Like the drug dog, Google's hashing system is trained (programmed) to find only the presence of a specific type of material, in this case an image file suspected of being contraband. *See* Richard P. Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 42-43 (2006). The system makes this determination without opening the email or image files – it looks only for the hash value, which Google's "computers can automatically recognize." ER:79. And once a match is made, Google automatically sends an electronic alert to NCMEC. There is no rummaging for what is suspected but unknown. There is only confirming the presence of what has previously identified as likely contraband.

Thus, while a hash match – like a dog alert – may provide probable cause to be used in applying for a search warrant, it is not itself a "search" under the Fourth Amendment. *See Place*, 462 U.S. at 707; *Illinois v. Caballes*, 543 U.S. 405, 409 (2005) ("the use of a well-trained narcotics-detection dog—one that 'does not

expose noncontraband items that otherwise would remain hidden from public view,'—during a lawful traffic stop, generally does not implicate legitimate privacy interests.") (citation omitted).[9]

Nor does it matter that a Google employee initially took part in generating the hash value that its software later used to automatically flag Mr. Wilson's image files. The fact that a human trains the dog to identify cocaine or marijuana does not transform the dog's alert into a search. This is equally true of the hashing technology used here. Although a human programed the software, the subsequent automated matching was no more a search than the dog-sniff.

b. *The private search doctrine does not apply to automated hashing software because only a human can frustrate another human's expectation of privacy*.

This point leads to another reason the private search doctrine is inapplicable – the absence of human participation. The idea of a reasonable expectation of privacy assumes a privacy interest vis-à-vis other humans. Only a human can violate another human's privacy – dogs don't read diaries. Thus, if no human knows what the computer found, privacy remains intact. And because the private search doctrine requires an initial, private frustration of an individual's privacy, *see Jacobsen*, 466

[9] This is not to say hashing will never constitute a search. The analysis might be different, for instance, if hashing were used to identify a non-contraband file – such as a photo of a political dissident or a protest – attached to an email. But that is not how Google's hashing was used in this case.

U.S. at 117, only when that private actor is a human (or the private search involves a human) can the doctrine apply. Indeed, no case of this Court or the Supreme Court has ever applied the doctrine to a machine search with no human involvement.

Accordingly, to do so here would be a radical departure; one that untethers the doctrine from its underlying rationale. There is no cause for such a departure. Thus, because the private search doctrine simply does not apply, it cannot excuse Agent Thompson's warrantless search.

3. The Supreme Court has repeatedly declined to extend other established warrant exceptions to technologies, like cell phones, that provide increased access to personal data.

This conclusion finds further support in *Riley v. California*, 134 S. Ct. 2473 (2014), and *Carpenter*. Both provide examples of the Supreme Court's unwillingness to extend well-worn Fourth Amendment doctrines in the face of technological innovations that allow greater privacy intrusions. *See Riley*, 134 S. Ct. at 2485 (declining to extend the search-incident-to arrest exception to searches of data on cell phones); *Carpenter*, 138 S. Ct. at 2217 (declining to extend the third-party doctrine to cell phone location records automatically generated and held by a third-party provider).

Riley provides a particularly apt comparison. In holding that a warrantless cell phone search could not be justified by the search-incident-to arrest exception, the Supreme Court explained: "First, a cell phone collects in one place many distinct

types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible . . . . Third, the data on a phone can date back to the purchase of the phone, or even earlier . . . . Finally, there is an element of pervasiveness that characterizes cell phones but not physical records." *Id.* at 2489-90.

These factors also apply to the email accounts. "Service providers offer many gigabytes of storage for free, so people have little incentive to delete email." Brief of Amicus Curiae (EFF Amicus), *United States v. Ackerman II*, No. 17-3238, at 6 (10th Cir. 2018) (available at https://www.eff.org/document/eff-et-al-amicus-brief-us-v-ackerman-10th-circuit-court-appeals-2018). In particular, "Google offers its email users 15 gigabytes of storage—the equivalent of about 150 yards of books on a shelf." *Id.* at n.2. "One study found that, on average, people have around 8,000 emails stored with their service provider, and about 20 percent of users have more than 21,000 emails stored in their inbox." *Id.* at 6-7. As in *Riley*, therefore, email accounts "differ in both a quantitative and a qualitative sense from other objects[.]" 134 S. Ct. at 2478. Thus, for this reason too, the judicially created private search doctrine should not be extended to email.

4. Assuming Google's hashing was a private search, Agent Thompson significantly expanded that search when he opened and viewed the image files.

However, assuming for the sake of argument that the doctrine did apply – i.e., that an automated, non-human hash match could be considered a search under the Fourth Amendment – it still would not advance the government's cause. Agent Thompson's opening and viewing the image files was a significant expansion on Google' hash match. It told the government much more than simply whether suspect images were actually contraband. A picture speaks a thousand words because it tells who, what, where and (often) when. A hash value, by comparison, says very little. It does not reveal any details, and cannot support a conviction.

As Agent Thompson admitted, he "wouldn't be able to compare [Google's hash value] against law enforcement's hash value databases[.]" ER:163. Rather, "[t]here would have to be some additional work" to determine what the image portrayed. ER:163. This added step violated the Fourth Amendment; it exceeded the scope of the private search.

a. *Walter controls.*

The Supreme Court reached exactly this conclusion in *Walter*. There, sealed packages containing boxes of film were delivered to the wrong company. *See Walter*, 447 U.S. at 651. Employees of the company opened the packages and examined the boxes – "on one side of which were suggestive drawings, and on the

other were explicit descriptions of the contents." *Id*. at 651-52. The employees then called the FBI, whose agents picked up the packages and, without consent or a warrant, "viewed the films with a projector." *Id*.

The Supreme Court held, "the unauthorized exhibition of the films constituted an unreasonable invasion of their owner's constitutionally protected interest in privacy. It was a search; there was no warrant; the owner had not consented; and there were no exigent circumstances." *Id.* at 654.

The Court explained: "the fact that that the packages and one or more of the boxes had been opened by a private party before they were acquired by the FBI [cannot] excuse the failure to obtain a search warrant." *Id.* at 656. Although the government claimed the "private search justified an unlimited official search," the argument failed because the agents "expan[ded] the private search." *Id.*

To this end, "the private party had not actually viewed the films. Prior to the Government screening, one could only draw inferences about what was on the films. The projection of the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search." *Id.* at 657. Moreover, "[t]he fact that the labels on the boxes established probable cause to believe the films were obscene clearly cannot excuse the failure to obtain a warrant; for if probable cause dispensed with the necessity of a warrant, one would never be needed." *Id.* at n.10.

The Supreme Court continued: "The private search merely frustrated [the expectation of privacy] in part. It did not simply strip the remaining unfrustrated portion of that expectation of all Fourth Amendment protection. Since the additional search conducted by the FBI – the screening of the films – was not supported by any justification, it violated that Amendment." *Id*. at 659. In other words, "[a] partial invasion of privacy cannot automatically justify a total invasion." *Id*. at n.13.

This reasoning applies with equal force here. The information provided by Google's automated hash review was not materially different than reading the descriptive material on the film boxes in *Walter*. Indeed, the hash value acted precisely like a descriptive label or a Dewey-decimal card. It told Google what the image file *likely* was, but did not reveal the *actual* image. Nor could the hash value be used to reverse-generate those images.

With nothing but the hash match and Google's "A1" code, Agent Thompson "could only draw inferences" without actually knowing what, specifically, would be revealed when he opened the image files. *Id*. at 657. By way of analogy, having a film box labeled "Casablanca" with a "PG" rating is strong evidence of what's inside, but it is not the same as watching the movie. So too with a hash match; it was "not sufficient to support a conviction." *Id.* at 654. Rather, "[f]urther investigation – that is to say, a search of the contents of the [images] – was necessary in order to obtain the evidence which was to be used at trial." *Id*.

This further investigation – opening and viewing the images file, just like viewing the films in *Walter* – violated the Fourth Amendment. And it did so "whether [the Court] view[s] the official search as an expansion of the private search or as an independent search supported by its own probable cause." *Id.* at 656. In short, Google's "partial invasion of privacy cannot [] justify [Agent Thompson's] total invasion." *Id*. at 659 n.13.

The district court, however, saw things differently. Relying heavily on *Jacobsen*, it concluded, "the government's expansion of Google's private search was not significant." ER:203. But *Jacobsen* is inapposite.

b. *Jacobsen is inapposite*.

In *Jacobsen*, FedEx employees opened a damaged package, found suspicious bags of white powder inside, and passed the parcel to the government. *See* 466 U.S. at 111. DEA agents repeated the same investigation, opening the package and examining its contents. *See id*. The agents also performed a chemical drug test to confirm the substance was cocaine. *See id*. at 111-12.

The Supreme Court upheld the search. It explained that, when the agents repeated the private search and revealed the block of white powder, their actions did not implicate the Fourth Amendment. *See id*. at 118. However, "[t]he question remain[ed] whether the additional intrusion occasioned by the field test . . . was an

unlawful 'search' or 'seizure' within the meaning of the Fourth Amendment." *Id.* at 122.

The Court held it was not. "A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy . . . . [G]overnmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest." *Id.* at 123. Thus, "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct." *Id.* at 126.

Here, the district court drew a direct line between the chemical test in *Jacobsen* and Google's hashing. ER:205 ("Compared to *Jacobsen*, there was even more of a 'virtual certainty' that SA Thompson could 'learn nothing that had not previously been learned during the private search.'") (citation omitted). On first blush, the comparison is understandable. But it fails on closer examination. Indeed, what happened here is much closer to *Walter* than *Jacobsen.* And *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013), proves the point.

i. *Keith* demonstrates that *Walter*, not *Jacobsen*, is controlling.

In *Keith*, AOL found a hash match in the defendant's email, and forwarded a CyberTipline report to NCMEC. *See id.* at 36-38. Unlike here, however, a NCMEC

employee actually opened the images before sending them to law enforcement. *See id.* at 37. The court explained that if the NCMEC employee had not opened the images but instead they had first been reviewed by law enforcement (as here), under *Walter*, "it could not seriously be contended that the law enforcement agency could open and inspect the contents of the file without regard to the Fourth Amendment's warrant requirement." *Id.* at 41-42.

"Although the media in which criminally obscene material was stored are different in *Walter* and this case, the pattern is the same. A label (here, hash value) that is examined without opening the film or file suggested the nature of the contents. For that reason, concerned private parties provided the film or file to the government without first reviewing the contents themselves. Government personnel then examined the contents of the film or file by opening and viewing it." *Id.* at 42. Under *Walter*, "the examination should not have been done without due compliance with the warrant requirement imposed by the Fourth Amendment." *Id.*

Nevertheless, "[t]he government weakly argue[d] that . . . viewing of the contents of the file was not an expansion of AOL's private search, citing *United States v. Jacobsen*[.]" *Id.* But "[a]n argument that *Jacobsen* is factually similar to this case is untenable in light of the [fact] . . . that AOL *forwarded the suspect file only because its hash value matched a stored hash value, not because some AOL employee had opened the file and viewed the contents*. The [government] expanded

the review by opening the file and viewing (and evaluating) its contents. *Walter*, and not *Jacobsen*, is the better analog." *Id.* at 42-43 (emphasis added).

"[M]atching the hash value of a file to a stored hash value is *not* the virtual equivalent of viewing the contents of the file. What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, but the provenance of that designation is unknown. So a match alone indicts a file as contraband but cannot alone convict it." *Id.* at 43 (emphasis added). Thus, "the actual viewing of the contents provides information additional to the information provided by the hash match. This is unlike what the Court found the case to be in *Jacobsen*, where the subsequent DEA search provided no more information than had already been exposed by the initial FedEx search." *Id.*

Plainly, *Keith*'s analysis is equally applicable here. And there are additional reasons *Jacobsen* is inapposite.

ii. This case is the opposite of *Jacobsen*.

As noted, in *Jacobsen*, the private party conducted the most invasive part of the search – opening the package and viewing its contents – thereby frustrating the reasonable expectation of privacy. Only the nonintrusive chemical test of the cocaine sitting in plain sight remained for the government. Here, it was the inverse.

Google performed the limited, non-invasive scan, which the government then expanded by opening and viewing the image files.

Another point of departure is that, in *Jacobsen*, both the FedEx employees and the government agents were staring at the same brick of white powder. They both knew exactly the same information about the powder's appearance – e.g., color, amount, texture, etc. The government's chemical test added only that the powder was in fact cocaine.

A comparable scenario under the facts of this case would be if a Google employee, followed by a government agent, viewed the images in Mr. Wilson's emails, but the agent then ran the file through a database to determine a potential hash match. In that circumstance, there would be no material expansion. But here, only the government agent opened the email files. And in doing so, he did not "merely disclose[] whether or not [the image was child pornography]." *Jacobsen*, 466 U.S. at 123. Agent Thompson also saw all the details, exactly what (and who) was portrayed, thereby gaining additional, valuable information he could use against Mr. Wilson in a criminal prosecution. Thus, while "no Fourth Amendment interest is implicated [when] the police have done no more than fail to avert their eyes," here, Agent Thompson's invasive gaze went much further. *Id.* at 130 (White, J., concurring).

Finally, the analogy to *Jacobsen* breaks down because, unlike a chemical drug test, a hash match does not provide a "virtual certainty" that the suspect file is necessarily an image that has been previously identified as child pornography. ER:205. To the contrary, as the Electronic Privacy Information Center (EPIC) recently explained in a similar case, "[t]here are at least three types of errors that could trigger the search and production of a Google user's personal data to law enforcement where no contraband image was ever uploaded." Brief of Amicus Curiae (EPIC Amicus), *United States v. Miller*, No. 18-5578, at 8-9 (6th Cir. 2018) (available at https://epic.org/amicus/algorithmic-transparency/miller/EPIC-Amicus-US-v-Miller.pdf).

- "First, a Google employee could mistakenly flag a non-contraband image (record entry error). Depending on a service provider's method for flagging images, it is possible that an employee could either flag the wrong image or mistakenly identify an image as apparent contraband when in fact the image does not contain contraband."[10]

- "Second, a service provider might erroneously flag an image based on a list of hash values that it received from some other entity (downstream error)."

- "Third, the flag from the provider's hashing algorithm could be a 'false positive' due to the specific image-matching method used (match error). A false positive could, for example, be caused by similarities in the images even if one image contains contraband and the other does not. The likelihood of a mismatch error

[10] To this end, here, the government has not provided any information about the reliability of the Google employee who allegedly created the initial hash value. *Cf. United States v. Cedano-Arellano*, 332 F.3d 568, 570-71 (9th Cir. 2003) (when the government relies on a narcotic detector dog to establish probable cause, it must provide discovery as to the dog's training and reliability).

> depends entirely on the specific hashing method used and its false positive rate. For example, certain file hashing algorithms are designed to confirm that when a copy of data is made, the original is unaltered and the copy is identical, bit-for-bit. But there is no evidence on the record that Google's proprietary image matching algorithm matches files bit-for-bit."

Id. (certain citations and quotation marks omitted).

Accordingly, because: (1) the government's opening and viewing the image files came after, and was more intrusive than Google's automated hashing, (2) unlike looking at the brick of cocaine, a Google employee did not see the alleged contraband in Mr. Wilson's email, and (3) the hash match cannot provide the same virtual certainty as a chemical test, the district court's reliance on *Jacobsen* was misplaced.

c. *Tosti is irrelevant.*

Nor is *United States v. Tosti*, 733 F.3d 816 (9th Cir. 2013), a better analog. In *Tosti*, the defendant took his computer to a store for service. *See id.* at 818. While repairing the computer, employees opened various folders containing child pornography images, which they viewed as thumbnails. *See id.* at 818-19. The employees contacted the police, who came to the store and viewed the images without first obtaining a warrant. *See id.*

The defendant argued the police violated the Fourth Amendment because they "viewed th[e] pictures not just as thumbnails, but also as enlarged pictures in a slideshow format." *Id.* at 822.

This Court rejected that argument: "[The police] did not exceed the scope of [the employees'] prior search because [the employees] and both detectives testified that they could tell from viewing the thumbnails that the images contained child pornography. That is, the police learned nothing new through their actions. Since [] — a private individual to whom Tosti had voluntarily delivered his computer with the explicit understanding that he would inspect the system to complete the repairs — could discern the content of the photos, any expectation of privacy Tosti had in those pictures was extinguished. Whether detectives later enlarged them (or the size of the enlargements, for that matter) is thus irrelevant." *Id.*

Here, however, *Tosti*'s entire discussion is irrelevant. No Google employee viewed the specific image files – as thumbnails or otherwise – in Mr. Wilson's email.

Accordingly, to the extent the private search doctrine applies, *Walter* remains the controlling precedent. And it serves only to confirm the Fourth Amendment violation.

D. The district court's erroneous reliance on the terms of service.

The district court also suggested Google's terms of service rendered Mr. Wilson's subjective expectation of privacy unreasonable. ER:199. Although the court stated it was not relying on this finding, ER:200, the government will surely ask this Court to affirm on that basis. But the district court's dictum was misguided.

The court's suggestion was rooted in the following provision of Google's terms of service: "Our Services display some content that is not Google's. This content is the sole responsibility of the entity that makes it available. We may review content to determine whether it is illegal or violates our policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law. But that does not necessarily mean that we review content, so please don't assume that we do." ER:82, 199.

Based on this provision, the district court found, "[Google's] monitoring policy regarding illegal content, which Defendant agreed to, rendered Defendant's subjective expectation of privacy in the four uploaded child pornography attachments objectively unreasonable." ER:199.

Google disagrees. It (and other ESPs) recently filed an amicus brief rejecting the district court's interpretation of its terms of service. Google maintains, "[t]he Fourth Amendment generally protects users' reasonable expectations of privacy in the contents of emails held by a third-party service provider from warrantless search and seizure by the government, irrespective of whether the service provider has terminated that user's account or *whether the user violated the terms governing his relationship with the service provider*." Brief of Amici Curiae (Google, et. al. Amicus), *United States v. Miller*, No. 18-5578, at 6-7 (6th Cir. 2018) (emphasis

added) (available at https://epic.org/amicus/algorithmic-transparency/miller/US-v-Miller-6th-Cir-Corp-Amicus-Brief.pdf).

This should resolve the issue in Mr. Wilson's favor. But there are other reasons too. As a starting point, the district court misread the portion of the terms of service on which it relied.

The paragraph it cited addressed content "display[ed]" by a Google service but created by a third-party "entity." ER:82. It was contained within a section addressing Google's ownership of its *own* services and intellectual property. ER:82. This is separate from the sections governing "Your Google Account," ER:82, and "Your Content in our Services," ER:83. In other words, the portion of the agreement on which the district court relied is not directed at individual users like Mr. Wilson.

Rather, the section governing an individual account is, "Your Content in our Services." ER:83. Nothing in that section talks about Google employees "reviewing" any personal content. To the contrary, it says, "[o]ur *automated* systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection." ER:83 (emphasis added). Thus, other than an automated scan for advertising purposes, the terms of service for individual users contains no agreement that Google can or will monitor email for illegal content. As such, by its plain language, Google's terms of service disprove the district court's interpretation.

But even putting aside the district court's misreading, its reasoning proceeded from a fundamentally flawed assumption. In its view, a boilerplate contract of adhesion, accepted by millions with a simple click (and certainly without reading) can wholly strip the users of their fundamental rights. That is troubling, dystopian, and turns the Fourth Amendment into a paper tiger. Thankfully, it is wrong.

As the EFF explains, "courts have routinely held that individuals have a reasonable expectation of privacy in their email held in accounts operated by third party providers, even when those providers can access emails pursuant to contractual terms of service." *EFF Amicus* at 4. The EFF aptly summarizes the state of the law:

- "Like the modern cellphone, email accounts today can contain 'a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate.' *Riley*, 134 S. Ct. at 2490 . . . . [E]mail is 'a form of communication capable of storing all sorts of private and personal details, from correspondence to images, video or audio files, and so much more.' *Ackerman*, 831 F.3d at 1304. 'Account,' the Sixth Circuit noted in *Warshak*, is a particularly 'apt word for the conglomeration of stored messages that comprises an email account, as it provides an *account* of its owner's life.' 631 F.3d at 284 (emphasis added)." *Id.* at 7.

- "Individuals enjoy an expectation of privacy in email despite the fact that third parties facilitate the sending and receiving of messages." *Id*. at 9. It follows, therefore, that "[t]erms of service provide a poor vehicle for determining an objective expectation of privacy. Fundamentally, they govern the relationship between the user and the provider, not the user and the government." *Id.* at 13. "[A]s the Sixth Circuit pointed out in *Warshak*, a term of service granting the 'right of access' or 'the mere *ability* . . . to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy.' 631 F.3d at 286-87 (emphasis in original)." *Id.* at 14.

- "If terms of service dictated expectations of privacy, private actors could unilaterally set the contours of Fourth Amendment protections. The expectation of privacy analysis is intended to describe 'well-recognized Fourth Amendment freedoms,' *Smith*, 442 U.S. at 740 n.5, not the interests of private businesses as advanced by form contracts." *Id.* at 14-15. Thus, "courts have declined to find private contracts dispositive of individuals' expectations of privacy." *Id.* at 15.

By way of example, in *United States v. Thomas*, 447 F.3d 1191, 1198 (9th Cir. 2006), this Court held the "technical violation of a leasing contract" was insufficient to vitiate an unauthorized renter's legitimate expectation of privacy in a rental car. And just last term, in *Byrd v. United States*, 138 S. Ct. 1518 (2018), the Supreme Court confirmed that understanding. It explained that, although an unauthorized driver "constitutes a breach of the rental agreement, and perhaps a serious one, [] the Government fails to explain what bearing this breach of contract, standing alone, has on expectations of privacy in the car." *Id.* at 1529.

The point is clear. Agreements between private parties are *between private parties*. They do not control the scope of Fourth Amendment protection from government action. Thus, as Google itself concedes, its terms of service could not – and certainly did not – vitiate Mr. Wilson's reasonable expectation of privacy in his email.

And even if they could, this would have no bearing on Mr. Wilson's property-based argument. On that issue, Google's terms of service confirm Mr. Wilson's superior interest: "what belongs to you stays yours," ER:83, which strongly supports

his trespassory claim. *See Carpenter*, 138 S. Ct. at 2242 (Thomas, J., dissenting) (suggesting that, under contract law, this clause in Google's terms of service establishes the user's property right).

This brings the Fourth Amendment analysis to an end. In summary, as a matter of property and privacy, Agent Thompson violated the Fourth Amendment when he opened and viewed the contents of Mr. Wilson's email without a warrant. Neither the private search doctrine nor Google's terms of service excuse that violation. Accordingly, the "answer to the question of what police must do before searching [email contents based only on a hash match] is accordingly simple—get a warrant." *Riley*, 134 S. Ct. at 2495.

E. Suppression is the remedy for the Fourth Amendment violation.

The final issue is remedy. Its resolution is straightforward. Because there was no warrant, no statute, and no binding appellate precedent authorizing Agent Thompson's unconstitutional search, the good faith exception cannot apply, and

suppression is required. *See Vasey*, 834 F.2d at 789-90; *United States v. Lara*, 815 F.3d 605, 613-14 (9th Cir. 2016).[11]

Vasey is controlling: "Officer Jensen conducted an illegal warrantless search and presented tainted evidence obtained in this search to a magistrate in an effort to obtain a search warrant. The search warrant was issued, at least in part, on the basis of this tainted evidence. The constitutional error was made by the officer in this case, not by the magistrate as in [*United States v. Leon*, 468 U.S. 897 (1984)]. The *Leon* Court made it very clear that the exclusionary rule should apply (i.e. the good faith exception should not apply) if the exclusion of evidence would alter the behavior of individual law enforcement officers or the policies of their department. Officer Jensen's conducting an illegal warrantless search and including evidence found in this search in an affidavit in support of a warrant is an activity that the exclusionary rule was meant to deter." 834 F.2d at 789 (citations omitted).

Here, like *Vasey*, Agent Thompson "conducted an illegal warrantless search and presented tainted evidence obtained in this search to a magistrate in an effort to

[11] In other cases, when a NCMEC employee has opened the image, courts have applied the good faith exception based on NCMEC's statutory authorization to review CyberTipline reports. *See e.g.*, *Keith*, 980 F.2d at 46 ("Congress has by statute given NCMEC's CyberTipline a significant role in the investigation and subsequent prosecution of child pornography crimes, and has directed that it be supported by government grants."). But that does not apply here, because a NCMEC employee did *not* open Mr. Wilson's email files, and there is no similar authorization for law enforcement agents.

obtain a search warrant." *Id*.; *see also United States v. Camou*, 773 F.3d 932, 945 (9th Cir. 2014) ("The Supreme Court has never applied the good faith exception to excuse an officer who was negligent himself, and whose negligence directly led to the violation of the defendant's constitutional rights."). As the district court found, "excising the tainted evidence from the affidavit would not support issuance of the search warrant for Defendant's email account." ER:207. Thus, all evidence from the initial illegal search, including that obtained via the tainted warrant, must be suppressed.

The Court, therefore, should reverse the denial of Mr. Wilson's suppression motion, and vacate his convictions.

II.
The district court structurally erred in failing to obtain a written jury waiver.

Separately, the Court should remand for a new trial because the district court structurally erred in failing to obtain a written jury waiver.

Even when no objection is raised below, this Court "review[s] the adequacy of a jury-trial waiver de novo." *United States v. Shorty*, 741 F.3d 961, 965 (9th Cir. 2013); *United States v. Laney*, 881 F.3d 1100, 1106 (9th Cir. 2018).

"A criminal defendant's right to a jury trial is fundamental." *United States v. Cochran*, 770 F.2d 850, 851 (9th Cir. 1985). However, a defendant may waive this right *if* the requirements of Federal Rule of Criminal Procedure 23(a) are satisfied.

See id. The rule provides: "If the defendant is entitled to a jury trial, the trial must be by jury unless: (1) the defendant waives a jury trial in *writing*; (2) the government consents; and (3) the court approves." Fed. R. Crim. P. 23(a) (emphasis added). Additionally, the waiver must be knowing and intelligent. *Cochran*, 770 F.2d at 851.

Although Rule 23 mandates a written waiver, courts have created (seemingly out of whole cloth) an exception, such that "under certain circumstances an oral waiver may be sufficient." *Shorty*, 741 F.3d at 966. To fall within this exception, "district courts [must] ensure that a jury trial waiver is knowing and intelligent by engaging in a substantial colloquy with defendants as well as informing them of four crucial facts: (1) twelve members of the community compose a jury; (2) the defendant may take part in jury selection; (3) jury verdicts must be unanimous; and (4) the court alone decides guilt or innocence if the defendant waives a jury trial." *Id.* (quoting *Cochran*, 770 F.2d at 853).

When the district court fails to "instruct[] the defendant of the four facts" it has not conducted "[a]n in-depth colloquy," "the waiver [is] invalid," and "[a]n invalid jury waiver is structural error." *Id*. at 966, 969.

Here, the district court failed to obtain a written waiver.[12] "As a result, [Mr. Wilson's] waiver is not presumed valid, and his oral waiver – his only waiver – is subject to greater scrutiny." *Id.* at 967. Under this greater scrutiny, "the court's colloquy prior to accepting [the] waiver was inadequate to ensure that [Mr. Wilson] understood the right he was waiving." *Id.* At most, "[t]he court instructed [him] on only two of the four facts required." *Id.* It told Mr. Wilson, "it would be required that all 12 jurors find you guilty." ER:219. This arguably covered part of fact 1 and fact 3 (the number of jurors and unanimity).

Mr. Wilson was not advised, however, that jurors come from his "community" (fact 1); that he could help choose the jury (fact 2); or the court alone decides guilt or innocence if he waived a jury trial (fact 4). Moreover, the district court misinformed Mr. Wilson that "if this case went to trial, you would have the right to have the jury decide whether or not you're *innocent* or *guilty*." ER:218-19 (emphasis added). But the jury is never asked to determine actual innocence.

---

[12] Under the plain language of Rule 23(a), this should end the inquiry and require reversal. Because this Court's oral waiver exception directly conflicts with Rule 23(a), it is invalid and should be overruled. *See United States v. Petri*, 731 F.3d 833, 839 (9th Cir. 2013) ("Because the Federal Rules of Criminal Procedure, once effective, have the force and effect of law, we apply 'traditional tools of statutory construction to interpret them.'") (citation omitted). Indeed, it is unfair that the Court strictly construes the writing requirement of Federal Rule of Criminal Procedure 11(a)(2) (conditional guilty pleas) against criminal defendants, *see United States v. Echegoyen*, 799 F.2d 1271, 1276 (9th Cir. 1986); *United States v. Cortez*, 973 F.2d 764, 766 (9th Cir. 1992), but not Rule 23(a) when it works to their benefit.

Making matters worse, the district court addressed the jury-waiver colloquy in the same breath as evidentiary stipulations. ER:219. In doing so, the court made it seem that the jury waiver was part of, and of the same character as, stipulating to certain facts. ER:219-20. This, of course, is inaccurate.

Finally, the district court took the oral waiver approximately two weeks before the trial. Thus, at the very least, it should have confirmed the waiver before proceeding. But that never happened. ER:231-32. Accordingly, "the district court did not fulfill its 'serious and weighty responsibility' of ensuring that [Mr. Wilson's] waiver was knowing and intelligent." *Shorty*, 741 F.3d at 968 (citation omitted).

Nor does it matter "that [Mr. Wilson] may have made a 'tactical choice' to waive a jury[,]" because this "tells [] nothing about whether he understood what he would be giving up by making such a choice. It was the district court's responsibility to fully inform [Mr. Wilson] of the nature and import of the right he was waiving, no matter his (or his counsel's) reason for waiving it." *Id.* at 969. That responsibility went unfulfilled. This Court, therefore, must reverse and remand. *Id.*

III.
The private search doctrine should be overruled.

For purposes of preservation, Mr. Wilson further contends the private search doctrine should be overruled: "The notion that private searches insulate from Fourth Amendment scrutiny subsequent governmental searches of the same or lesser scope

is inconsistent with traditional Fourth Amendment principles." *Walter*, 447 U.S. at 660 (White, J. and Brennan, J., concurring). Moreover, the doctrine is untenable under a property-based analysis. *See Ackerman*, 831 F.3d at 1307 (noting "the uncertain status of *Jacobsen* after *Jones*").

CONCLUSION

The district court erred in denying Mr. Wilson's motion to suppress and in failing to obtain a written waiver of his right to a jury trial. To remedy these errors, this Court should vacate his convictions.

Respectfully submitted,

s/ Devin Burstein

Dated: March 21, 2019

Devin Burstein
Warren & Burstein
501 West Broadway, Suite 240
San Diego, Ca. 92101

CERTIFICATE OF RELATED CASES

Counsel for the Appellant is unaware of any related cases pending before this Court, which should be considered in this appeal.

Respectfully submitted,

s/ Devin Burstein

DATED: March 21, 2019

DEVIN BURSTEIN
Attorneys for Defendant-Appellant

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 18-50440

I am the attorney or self-represented party.

This brief contains 13,263 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[X] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[ ] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
- [ ] it is a joint brief submitted by separately represented parties;
- [ ] a party or parties are filing a single brief in response to multiple briefs; or
- [ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature *s/ Devin Burstein* **Date** 03/21/2019
(use "s/[typed name]" to sign electronically-filed documents)

ADDENDUM

TABLE OF CONTENTS

Federal Rules

ADDENDUM A

United States Code Annotated
Federal Rules of Criminal Procedure for the United States District Courts (Refs & Annos)
VI. Trial

Federal Rules of Criminal Procedure, Rule 23

Rule 23. Jury or Nonjury Trial

Currentness

(a) Jury Trial. If the defendant is entitled to a jury trial, the trial must be by jury unless:

(1) the defendant waives a jury trial in writing;

(2) the government consents; and

(3) the court approves.

(b) Jury Size.

(1) In General. A jury consists of 12 persons unless this rule provides otherwise.

(2) Stipulation for a Smaller Jury. At any time before the verdict, the parties may, with the court's approval, stipulate in writing that:

(A) the jury may consist of fewer than 12 persons; or

(B) a jury of fewer than 12 persons may return a verdict if the court finds it necessary to excuse a juror for good cause after the trial begins.

(3) Court Order for a Jury of 11. After the jury has retired to deliberate, the court may permit a jury of 11 persons to return a verdict, even without a stipulation by the parties, if the court finds good cause to excuse a juror.

(c) Nonjury Trial. In a case tried without a jury, the court must find the defendant guilty or not guilty. If a party requests before the finding of guilty or not guilty, the court must state its specific findings of fact in open court or in a written decision or opinion.

CREDIT(S)

(As amended Feb. 28, 1966, eff. July 1, 1966; Apr. 26, 1976, eff. Oct. 1, 1977; Pub.L. 95-78, § 2(b), July 30, 1977, 91 Stat. 320; Apr. 28, 1983, eff. Aug. 1, 1983; Apr. 29, 2002, eff. Dec. 1, 2002.)

Fed. Rules Cr. Proc. Rule 23, 18 U.S.C.A., FRCRP Rule 23
Including Amendments Received Through 3-1-19